WN 98W000032

MITRE REPORT

A Study of the Defense Simulation Internet (DSI) for the Joint Advanced Distributed Simulation (JADS) Project

April 1998

Devaraj Sahu

MITRE
Washington C³ Center
McLean, Virginia

Approved for public release.

Abstract

This report investigates the feasibility of the recently upgraded Defense Simulation Internet (DSI) network to support Test and Evaluation (T&E) requirements such as the Joint Advanced Distributed Simulation (JADS) phase two end-to-end (ETE) test. It reviews the features associated with the DSI and discusses how the DSI could be used to support JADS ETE T&E efforts.

The DSI provides for bandwidth reservation among its user sites through the use of standards-based Resource ReSerVation Protocol (RSVP). Multicasting is supported so that packets in a distributed simulation are efficiently forwarded. Security is provided by Improved Network Encryption System (INES) boxes built by the Motorola Corporation. Desktop Video Teleconferencing (DVTC) applications can be used among limited number of sites in secure or non-secure mode.

A JADS Phase two ETE test configuration for T&E is discussed and a potential configuration for running this test over DSI is presented. Because of the throughput limitations of the INESs (maximum two-way throughput being 1200 Kbits per second), it is suggested that running JADS ETE phase two tests over the DSI is not a viable option at the present time.

Table of Contents

Section 1

1. INTRODUCTION

The Joint Advanced Distribution Simulation (JADS) program is chartered by the Office of the Secretary of Defense (OSD) to investigate the utility of Advanced Distributed Simulation (ADS) for Test and Evaluation (T&E) applications. JADS has also been asked to identify ADS constraints and methodologies when used for T&E and to identify requirements for ADS systems to better support T&E in the future (for more information, see their web page: www.jads.abq.com/html/jads).

The JADS Joint T&E project consists of three multi-phased test programs: the System Integration Test (SIT), End-to-End (ETE) test, and finally Electronic Warfare (EW) test. The SIT test has been scheduled to run from 1995 through 1998 and the EW and ETE tests will run through 1999. For each phase of a given test program, there is an associated test scenario that defines a prescribed set of interactions among the program entities. For JADS T&E efforts, a key element of the test program is the communications infrastructure that supports the execution of a test scenario.

The JADS Test Director has requested that MITRE investigate the feasibility of the recently modernized Defense Simulation Internet (DSI) to support T&E requirements, such as those represented by the SIT, ETE, and EW tests. In response, MITRE's Networking and Communications Engineering Center initiated a study of the upgraded DSI and its potential impact on JADS-based T&E. This paper reviews the features associated with the DSI and looks at one phase of the JADS ETE test program and discusses how DSI could be used to support this test. This paper also examines the cost and performance implications of using the DSI in the test.

1.1 BACKGROUND

The DSI is a network that allows distributed simulations from all branches of the military to interoperate. It is owned by the Defense Information Systems Agency (DISA). The old DSI (Phase I) wide area network (WAN) consisted of out-dated equipment such as Bolt Beranek and Newman (BBN) T/20 routers and proprietary implementations of the Streams Protocol, Version II (ST II). The modernized Phase II DSI replaced these with state of the art equipment and standards-based commercial products.

1.2 PURPOSE

In this report, the technical characteristics of the modernized DSI network are examined in detail and include the standards-based protocols and applications available in the network. Understanding these characteristics is important in evaluating the feasibility of the DSI

network to support Advanced Distributed Simulation (ADS) T&E efforts. The JADS ETE test is one such effort that is representative of that performed by T&E personnel. In this paper we examine the issues and the feasibility of running a JADS ETE test over the DSI. The issues can be broadly characterized as technical and managerial. The technical issues are: bandwidth, latency, and resource availability to run JADS ETE tests. The managerial issues are: costs, node locations, and exercise scheduling.

1.3 SCOPE

This report has a limited scope. It provides a short summary of the capabilities of the Phase II DSI. It gives simple examples, where appropriate, to provide the JADS community with a better feel for its features and capabilities. This report examines a JADS ETE test scenario that can be run over the DSI. Studying all the ETE test scenarios is beyond the scope of the present paper. Cost estimates are generally reliable; however, they should be confirmed to avoid surprises.

1.4 DOCUMENT ORGANIZATION

In Section 2, the DSI Phase II network is described in detail. Section 3 describes the JADS ETE test scenario and a possible DSI set up that could support the JADS test. Advantages and disadvantages of running JADS over DSI are presented. Section 4 presents the conclusions of this study. Appendixes present detailed information, such as, router configurations, and physical connectivity of VTC equipment.

Section 2

2. DSI PHASE II

The Phase II upgrade of the DSI was completed in October 1997. With this upgrade the DSI transitioned from proprietary products to standards-based products. In this section, the DSI topology and capabilities are discussed. These capabilities include: Resource ReSerVation Protocol (RSVP), multicasting, routing, video-teleconferencing (VTC), security, and network management. DSI membership information and future upgrade plans are discussed towards the end.

2.1 TOPOLOGY

The DSI backbone has seven nodes arranged in a partial mesh topology (Figure 1). Each node consists of a Cisco 7500 router connected to a Defense Information Systems Network (DISN) ATM Switch (not shown). Each of these switches, in turn, is connected to a commercial ATM cloud which provides 3 Megabits per second (Mbps) permanent virtual circuit (PVC) pipes among the nodes.

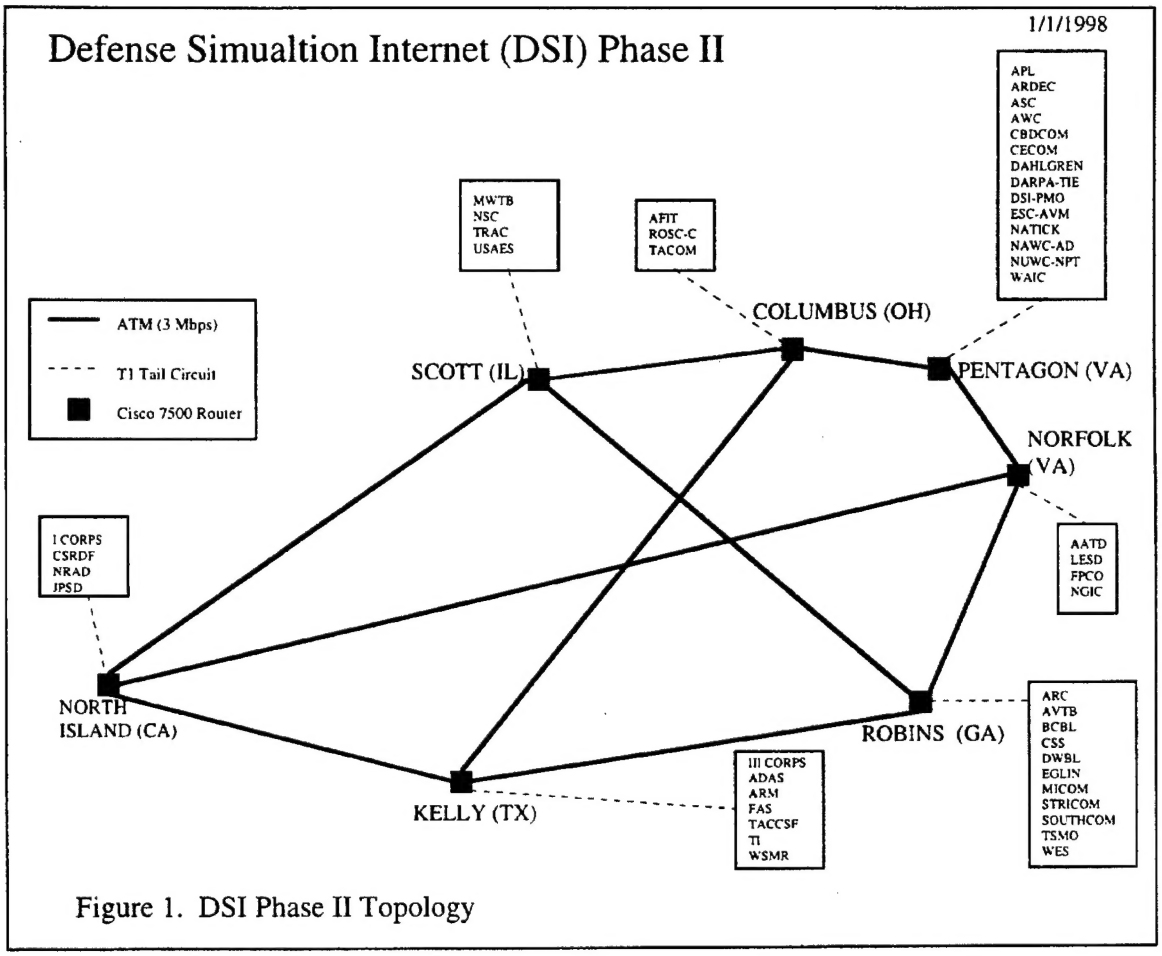


Figure 1. DSI Phase II Topology

The IP address assignments and the ATM connection identifiers such as Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) of the backbone ATM interfaces are shown in Figure 2.

Back Bone Node	IP Address / Mask 199.57.64.X / 30	Interface	Description	VPI, VCI
COLUMBUS	98	ATM0/0.1	To PENTAGON	0, 103
COLUMBUS	85	ATM0/0.2	To KELLY	4, 121
COLUMBUS	89	ATM0/0.3	To SCOTT	10, 120
KELLY	117	ATM0/0.1	To NORTH ISLAND	37, 122
KELLY	114	ATM0/0.2	To ROBINS	41, 126
KELLY	86	ATM0/0.3	To COLUMBUS	4, 121
NORFOLK	94	ATM0/0.1	To PENTAGON	0, 101
NORFOLK	101	ATM0/0.2	To ROBINS	49, 127
NORFOLK	105	ATM0/0.3	To NORTH ISLAND	0, 101
NORTH ISLAND	118	ATM0/0.1	To KELLY	37, 122
NORTH ISLAND	106	ATM0/0.2	To NORFOLK	39, 125
NORTH ISLAND	121	ATM0/0.3	To SCOTT	6, 124
PENTAGON	93	ATM0/0.1	To NORFOLK	0, 101
PENTAGON	97	ATM0/0.2	To COLUMBUS	0, 103
ROBINS	109	ATM0/0.1	To SCOTT	5, 123
ROBINS	113	ATM0/0.2	To KELLY	41, 126
ROBINS	102	ATM0/0.3	To NORFOLK	43, 127
SCOTT	110	ATM0/0.1	To ROBINS	5, 123
SCOTT	122	ATM0/0.2	To NORTH ISLAND	6, 124

Figure 2. IP Address Assignments of ATM Interfaces

Each backbone node is connected to several site nodes. There are a total of 46 tail sites at the present time. Each site node has a Cisco 7204 router with a serial T1 (1.54 Mbps) link to its backbone node. As an example, the configuration of one site (the Joint Precision Strike Demonstration (JPSD) site at Fort Huachuca, Arizona) is shown in Figure 3. We will also describe this configuration below.

Typically, a site router has one serial port and four Ethernet ports. One Ethernet interface is assigned a class C Internet Protocol (IP) address range for unclassified simulations. A single host IP address is available for desktop VTC (DVTC) via a second Ethernet interface. A third Ethernet segment connects to a port of the Improved Network Encryption System (INES) box built by the Motorola Corporation. This box helps in providing secure simulations and secure DVTC. Again, there is a complete class C IP address range for secure simulations and a single IP host address for secure DVTC. The simulation Local Area Network (LAN) and the DVTC LAN are connected to two Ethernet ports of a Cisco 4500 router on the red side (classified side). The maximum throughput from the INES is about 1.2 Mbps in both directions (combined) and is achieved by sending large packets (1400 Byte packets) through the INES. For smaller packets, the throughput is much smaller. To overcome this limitation, an aggregator box (which is a Personal Computer (PC) with a Pentium processor running on Free Berkeley System Distribution (BSD) operating system) connects to a third Ethernet interface of the Cisco 4500 router and an INES port (see Figure 3). Multicast traffic from the red side is packaged by the aggregator into larger packets and is shipped to the network via its black site router. Similarly multicast traffic destined for the red side is deaggregated and forwarded to the simulation LAN.

JPSD

FT. HUACHUCA, AZ

MODIFICATION DATE
25 SEP 97

EFFECTIVE DATE
25 SEP 97

Dial-In Phone:
Ckt ID:

POC#1 Robert A. Olson
Phone: 520-533-4612
FAX: 520-533-4605
Email:rob@huachuca-simcenter.army.mil

POC #2:
Ph#

Logistics:
Ph#

Property Book Officer:
Ph#

COMSEC SHIPPING ADDRESS:

SHIPPING ADDRESS:

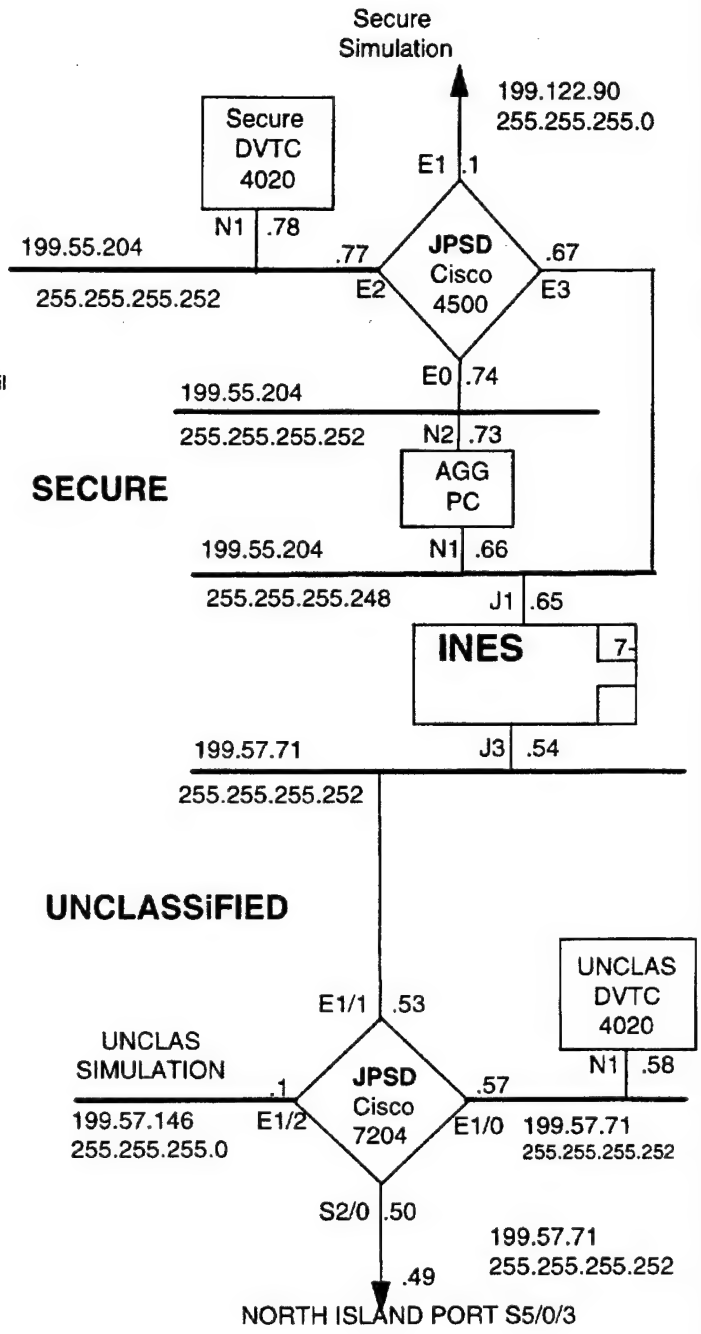


Figure 3. DSI Site Configuration

2.2 CAPABILITIES

The DSI phase II network supports standards-based protocols such as RSVP and H.320 VTC. In addition, the DSI network supports IP multicasting, link-state routing, secure and non-secure distributed simulations, and the usual internet and intranet applications such as file transfer, e-mail, telnet, and web-browsing. We highlight the main capabilities in the following subsections.

2.2.1 RSVP

The RSVP protocol reserves bandwidth for traffic moving from a source to a destination. Without RSVP, all traffic is treated on a best-effort basis. If the network is over-loaded, then packets in the traffic are dropped. With the invocation of RSVP, mission critical traffic is not dropped.

Request for Comment 2205 (RFC 2205) published by the Internet Engineering Task Force (IETF) lays down the functional specifications of RSVP. It states, "RSVP provides receiver-initiated setup of resource reservation for multicast or unicast data flows, with good scaling and robustness properties." The basic model of RSVP includes a sender application, that generates data, and a receiver application (or multiple receiver applications) that wishes to receive data. The sender transmits path messages downstream toward the receiver. This message is used to inform intermediate routers and the receiver (or group of receivers) about the characteristics of the path (such as bandwidth, delay, etc.) to be setup between the sender and the receiver. Based on this information, the receiver makes a reservation request and passes it upstream through the intermediate routers toward the source. At each intermediate router, the request is passed to admission control and policy control. Admission control checks to see if the node has sufficient available resources to grant the requested Quality of Service (QOS), and policy control checks to see if the user has permission to make the reservations. Both checks must be positive to reserve the necessary resources.

For applications that are not RSVP-capable, Cisco edge routers can be manually configured to install a reservation from a sender to a receiver. In order to successfully install a reservation through the network, all the intermediate routers must allocate RSVP bandwidths. If a link in the reservation chain is accidentally broken, then the reservation can be dynamically re-established via an alternate path, if resources along that path are available.

Some practical examples of making reservations in the DSI network are shown below.

- To setup a unicast reservation of 150 Kbps between a sender router A (IP address 199.57.127.10 and Ethernet interface Eth1/1) and a receiver router B (IP address 199.57.127.22 and Ethernet interface Eth2/1) the following configurations are entered in the routers.

  Router A (interface Ethernet1/1):

ip rsvp sender 199.57.127.22 199.57.127.10 UDP 0 0 199.57.127.10 Eth1/1 150 60

This statement sets up a path message from router A to router B using the user datagram protocol (UDP) with unassigned destination and source port numbers (0 0). A bandwidth of 150 Kbps is reserved for data flowing from the sender to the receiver with minimum burst size not exceeding 60 Kbps.

Router B (interface Ethernet2/1):

ip rsvp reservation 199.57.127.22 199.57.127.10 UDP 0 0 199.57.127.22 Eth2/1 ff load 150 60

This statement sets up a reservation message from the receiver to the source. The sender command on router A and the reservation command on router B jointly install a 150 Kbps reservation from A to B. This reservation is a fixed filter *(ff)* type implying that there is a single sender.

- To setup a native multicast reservation to the group 224.1.2.3 consisting of routers A (IP address 199.57.127.10 and Ethernet interface Eth1/1), B (IP address 199.57.127.22 and Ethernet interface Eth2/1), and C (IP address 199.57.125.15 and Ethernet interface Eth2/0), the following configurations are entered in the routers.

  Router A (interface Ethernet1/1):

  ip rsvp sender 224.1.2.3 199.57.127.10 UDP 0 0 199.57.127.10 Eth1/1 250 60

  ip rsvp reservation 224.1.2.3 0.0.0.0 UDP 0 0 199.57.127.10 Eth1/1 wf load 500 60

  The first statement sets up a path message from router A to the multicast group 224.1.2.3 using the UDP protocol with unassigned destination and source port numbers (0 0) with bandwidth 250 Kbps and the maximum burst size of the data not exceeding 60 Kbps. The second statement means that reservation messages from receivers in the multicast group come from all senders (address 0.0.0.0) and that the wild card filter (wf) reservation style applies.

  Router B (interface Ethernet2/1):

  ip rsvp sender 224.1.2.3 199.57.127.22 UDP 0 0 199.57.127.22 Et21/1 250 60

  ip rsvp reservation 224.1.2.3 0.0.0.0 UDP 0 0 199.57.127.22 Eth2/1 wf load 500 60

  The first statement sets up a reservation message from router B to router A. This reservation is a fixed filter *(ff)*.

  Router C (interface Ethernet2/0):

  ip rsvp sender 224.1.2.3 199.57.125.15 UDP 0 0 199.57.125.15 Eth1/1 250 60

ip rsvp reservation 224.1.2.3 0.0.0.0 UDP 0 0 199.57.125.15 Eth1/1 wf load 500 60

In addition, the statement *ip igmp join-group 224.1.2.3* should be inserted in the serial network interface of each of the routers A, B, and C.

2.2.2 Multicasting

Multicasting allows users to be members of a group of users and exchange traffic among themselves in an efficient manner. Membership in the group is activated through the Internet Group Management Protocol (IGMP). In addition, a routing protocol is needed to route traffic among its members. In the DSI, the protocol independent multicasting (PIM) dense-mode is used as the multicast routing protocol.

There are two modes of operations for multicast traffic. These two multicasting modes provide the DSI users with advanced features to run their applications among the participants in a test event. The first is a native multicasting, where an IP address range of 224.x.x.x to 254.x.x.x (where each x can be any number from 1 to 254) is used to indicate membership in the group. In native multicasting, packets are sent directly from a sender to a group of receivers. An example of reserving bandwidth for native multicasting was presented in the previous subsection. The DSI supports native multicasting applications such as VAT, which is an audio conferencing tool, and VIC, which is a video teleconferencing tool, and WB (white board), which is a chalk-board writing tool, all developed at the Lawrence Berkeley Laboratory. In addition, UDP traffic can be exchanged among members in the DSI. If the links, over which such UDP traffic is transmitted are congested, then packets could be dropped. However, if bandwidth is reserved for multicast flows, the UDP traffic will be protected.

The second mode of multicasting supported in the DSI is multicasting via subnet-directed broadcasting. This mode is useful for hosts that talk to each other by broadcasting a protocol data unit (PDU) to their local Ethernet. One such application is ModSAF (Modular Semi-automated Forces) which generates simulation entities and floods its local Ethernet with simulation PDUs. These entities then interact with entities generated by other hosts that participate in the distributed simulation exercise. The Cisco routers support a broadcast-to-multicast (and multicast-to-broadcast) functionality that allows routers to forward LAN traffic with time-to-live *(ttl)* scope of more than one router hop. An example of this "subnet-directed multicasting" configuration is given below, to give the readers a flavor of this advanced feature.

- Let the router A's Ethernet interface Eth1/1 (IP address 199.57.127.10) be connected to the LAN segment to which the ModSAF host is also attached (IP address 199.57.127.11). Let the serial interface S1/0 of router A be connected to the network.

Then the following statements are needed:

(interface Eth1/1)

ip multicast helper-map broadcast 224.1.2.3 100 ttl 10

(interface S1/0)

ip multicast helper-map 224.1.2.3 199.57.127.255 100

The first statement takes broadcast packets and forwards them to the group address 224.1.2.3 with access list of 100 and *ttl* of 10. The second statement accepts packets from the group 224.1.2.3 and broadcasts them to the Ethernet LAN to which the ModSAF host is attached.

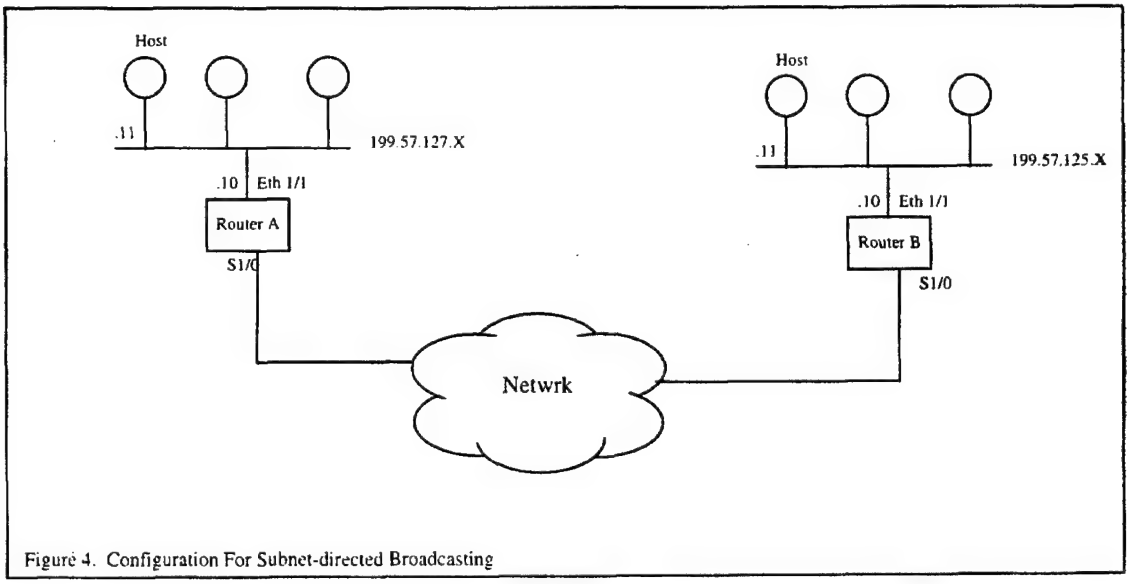


Figure 4. Configuration For Subnet-directed Broadcasting

2.2.3 Routing

The link-state protocol Open Shortest Path First (OSPF) is used for routing table updates within the DSI network. The network is partitioned into eight areas (area 0 through area 7). The backbone area is designated as area 0 with network address 199.57.64.0 and mask 255.255.255.0. The site areas are designated as area 1 through area 7 and share routing advertisements with the backbone area 0. Appendix A shows the OSPF configuration for the Norfolk backbone node, which belongs to area 2. The OSPF configuration for the Cisco 7204 site router at JPSD, which is linked to the North Island node and is part of area 7, is shown in Appendix B.

The Norfolk backbone router has an Ethernet link to the DISA Joint Information Services (JIS) router, which has connectivity to the Internet. The JIS router runs Cisco's proprietary Inter-gateway Routing Protocol (IGRP) and Enhanced-IGRP (EIGRP) in its routing domain. The IGRP autonomous system number is 568 for the JIS router. The DSI Norfolk router and the JIS router share routing updates via the Border Gateway Protocol 4 (BGP4) protocol. As shown in the BGP configuration in Appendix A, all the BGP advertisements for the entire DSI network are compactly done through the use of Classless Inter Domain Routing (CIDR) address blocks, beginning at 199.57.64.0 and 199.57.128.0 with their associated masks.

The routing for secure simulations and DVTC is done via default routing and a typical red Cisco 4500 configuration is shown in Appendix C. Further discussions of security aspects will be done in the security subsection.

The routing protocols in the DSI network are robust and have been thoroughly tested to prevent route-flapping and looping. OSPF and BGP provide state-of-art routing in the DSI network

2.2.4 VTC

DSI provides DVTC service among user sites with a maximum of four participants per session. The VTC equipment at a site consists of an Intel Pentium Personal Computer (PC) running the Windows 95 operating system installed on a removable hard drive. There are two identical removable hard drives of capacity one Gigabyte each. One hard drive is used for unclassified (black) VTC and the other for classified (red) VTC. A monitor, a pair of stereo speakers, and a camera are also included. The software for VTC and video-sharing are provided by Zydacron and PictureTel and integrated by Summit Solutions. The H.320 series of standards are used. These standards lay down the rules to transmit video/voice/data over Integrated Services Digital Network (ISDN) lines. Summit Solutions has developed a solution to convert the ISDN packets into Ethernet frames and then forward them to their destination. The frames can be transmitted at 64 Kbps through 384 Kbps in increments of 32 Kbps. There is an overhead of about 100 Kbps per frame, regardless of its payload. The emerging H.323 standards are expected to provide true packetized video over IP.

Point-to-point DVTC between any two video-equipped sites can be initiated. This is done by configuring the host IP address and the gateway IP address on the PC and by dialing a phone number in the database. White board, chat sessions, picture and file sharing can be invoked by the participants. For multiple participants in the VTC, RadVision's Gateway and Multipoint Control Unit (MCU) video-server units are needed. The MCU allows sessions among four participants and may be initiated by the Network Control Center (NCC) at Columbus, Ohio, where the MCU and the Gateway are configured. The MCU has four ports which connect to four ports of the Gateway which also has four Ethernet ports. These Ethernet ports are connected to four Ethernet ports on the Columbus backbone router (see

Appendix D). The participants request a conference ahead of time so that appropriate bandwidth may be reserved on the network for a successful video session.

The DVTC equipment is not only economical compared to bulky room system video that it replaced, but also provides additional savings by using the same equipment for both classified and unclassified work (except for the removable hard drive).

2.2.5 Security

Secure simulations and secure VTC may be done from the red side of a DSI site. The secure equipment consists of a Cisco 4500 router, a PC aggregator, VTC equipment, and an Improved Network Encryption System (INES) box manufactured by the Motorola Corporation. The INES provides DSI with end-to-end encryption. All the INES devices are administrated by an INES Enhanced Product Server (EPS) that does the following: configuration management, auditing, and electronic key management.

The INES is endorsed by the National Security Agency (NSA) to handle classified data up to the TOP SECRET level. However, for the DSI, it is authorized to handle only SECRET information. The INES provides for data confidentiality, data integrity, peer identification, and access control on the DSI. The INES has an unclassified LAN interface port (J3) that is connected to the unclassified network (black side). It has a classified LAN interface port (J1) that is connected to the classified network (red side). A key-shaped plastic case called KSD-64A (Key Storage Device) is used to store the following: a non-forgeable certificate, INES security platform identity, security classification, and an ASCII (American Standard Code for Information Interchange) identity. In addition to KSD-64A, a configuration floppy disk is needed to make the INES operational. At start up time the INES reads data on KSD-64A and stores it in non-volatile read-only memory (NVROM). The INES erases the KSD-64A, then creates and writes a Crypto Ignition Key (CIK) to it. The INES also calculates a cryptographic checksum for each file on the floppy disk. The INES writes a file called VERIFY.REC, that contains the checksum, to the floppy disk. In order to operate, the INES must have all the three parts mentioned above: the key data in NVROM, the CIK on KSD-64A, and the VERIFY.REC file on the floppy.

The INES takes packets forwarded to its red interface, encrypts the data, appends an IP header for transport across a black IP network, and ships them to the next-hop router. When an INES receives an encrypted packet, it decodes the packet and forwards to the red interface. For unicast sessions between a pair of INESs, a session key is established via a negotiation process between the pair. The INES maintains a table of session keys. For a multicast session, a multicast session key is established. As mentioned in section 2.1, the PC aggregator provides for better throughput for multicast traffic. The multicast traffic is forced to travel through the aggregator box via default route statements in the Cisco 4500 router, whereas the unicast traffic is default-routed to avoid the PC aggregator. A typical router configuration on the red side is given in Appendix C. Because of data encryption on the red

side, bandwidth reservation is not feasible. However, the traffic on the black side (unclassified side) can be reserved by invoking RSVP.

Multiway DVTC on the red side is scheduled with the help of 4 INESs, a Radvision Gateway, and a MCU at the Columbus backbone node. The black sides of the INESs are interfaced with 4 Ethernet ports on the Columbus backbone router.

2.2.6 Network Management

Network management functions are performed at the Network Control Center (NCC) at Columbus. Network controllers monitor backbone and site routers and circuits. They also provide help desk and trouble-shooting service, and set up exercises that are scheduled. The toll-free support number for the NCC at Columbus is 1-888-281-3286. The controllers use Hewlett-Packard Openview software (version 4.1.1) on a Solaris platform, in the black side, to assist them in monitoring faults and generating alarms. The current controllers, their phone numbers, and e-mail addresses are given in Appendix E:

In addition to the commercial tool mentioned above, a set of automated tools have been developed for the DSI. A user can use these tools to view incoming and outgoing traffic statistics at the site router. Authorized users can use the friendly interface provided by the tools to make unicast and multicast bandwidth reservations, configure router interfaces, view IP address assignments of all the routers, and view the up-down status of router interfaces. The tools also enable the controllers to reload all the router configurations automatically at a specific date and time and check for duplicate address assignments.

2.3 DSI MEMBERSHIP

Membership in the DSI community may be requested from DISA. The point of contact is Mr. T. Shannon at 703-735-8064 whose e-mail address is shannont@ncr.disa.mil. Another point of contact is Ms. Alice Bontrager at Columbus at 614-692-9138 whose e-mail address is bontragera@crcc.disa.mil. There is also a group e-mail address, dsicell@crcc.disa.mil that may be contacted for membership. Approximate cost for joining the DSI as a site node (at the time this report was written) is about *$60K* for equipment and about *$9K* per month for a T1 circuit charge. One Cisco 7204 router, one Cisco 4500 router, one INES, one PC aggregator, and one DVTC box with monitor and accessories are provided by DISA. The site is attached by a T1 tail circuit to one of the 7 backbone nodes. The backbone provides ATM PVC pipes of 3 Mbps among the 7 nodes in a partial mesh topology, as already mentioned.

2.4 FUTURE PLANS

Future upgrade plans for the DSI network include acquiring New INESs from the Motorola Corporation to increase throughput and decrease latency. H.323 compliant DVTC products and hardware-based codecs might also be acquired when they become available.

Section 3

3. JADS

In the previous section, we presented the characteristics, capabilities, and accessing information of the modernized DSI. The JADS Test force is interested in finding out if they can be part of this network and run their simulations. If this is feasible, then the T&E community can access DSI nodes and DSI simulation systems.

In this section we discuss a JADS ETE test configuration for T&E, a potential configuration for running this test over the DSI, and an evaluation of the DSI's suitability to support this test.

3.1 ETE TEST CONFIGURATION

The JADS ETE test consists of four phases. Phase 1 is a developmental phase in the laboratory that develops and integrates hardware and software for the test. Phase 2 is a phase (also in the laboratory) that tests the feasibility of ADS to support developmental T&E (DT&E) and operational T&E (OT&E). Phase 3 examines the interoperability of ADS with Joint Surveillance Target Attack Radar System (STARS) equipment. Finally phase 4 is a live test in which an actual airborne E-8C radar aircraft is linked to receivers and other systems on the ground.

In this report, the phase 2 test configuration is examined in detail. The network supporting this test scenario consists of five nodes: the Test, Control, and Analysis Center (TCAC) node located at Albuquerque, New Mexico; and four other nodes at: Fort Hood (III Corps), Texas; White Sands Missile Range (WSMR), White Sands, New Mexico; Grumman Aerospace Laboratory, Melbourne, Florida; and Fort Sill, Oklahoma. In this network, the TCAC is connected by dedicated T1 links to the other 4 nodes. In addition, the Joint STARS ground station at Grumman is connected to the ground station at Fort Hood by a simulated Surveillance and Control Data Link (SCDL) at a T1 rate. Test control among participating sites is done via one voice channel out of T1 link. A topology of the phase 2 ETE test scenario is shown in Figure 5.

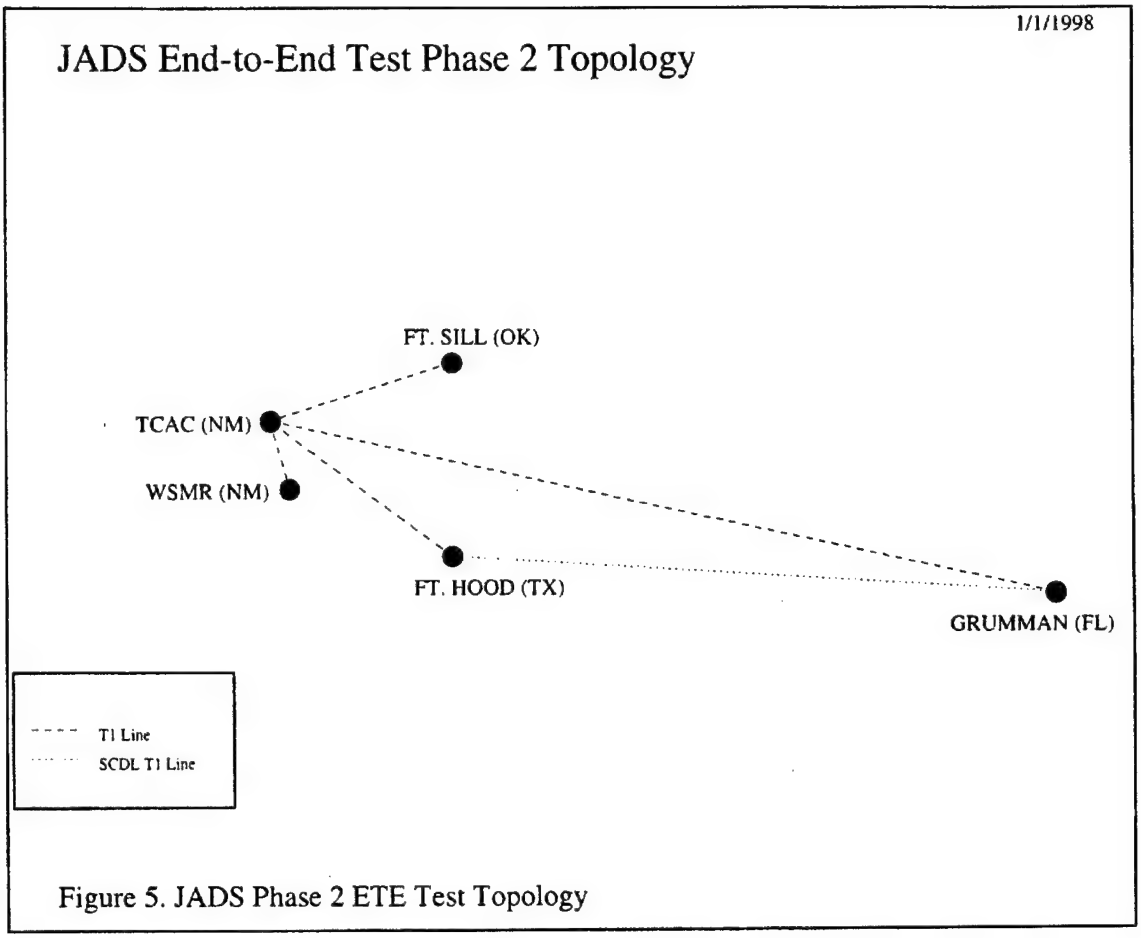


Figure 5. JADS Phase 2 ETE Test Topology

The network baseline requirements for running the JADS ETE phase 2 test on the DSI are derived from engineering analysis of expected data traffic. The derived requirements are (based partly on correspondence with JADS ETE Test Team Lead Lt. Col. Mark McCall):

1. The bandwidth (including voice) utilized in any given T1 link should not exceed that of 1/2 of a T1 link.
2. The aggregate bandwidth exceeded that of a T1 link but did not exceed that of a dual T1 link.
3. The upper limit of latency including allowable errors and radar timelines should be no longer than a second.

4. The exercises are classified.

3.2 JADS ETE TEST OVER DSI

A potential configuration for running a phase 2 ETE test over the DSI is shown in Figure 6.

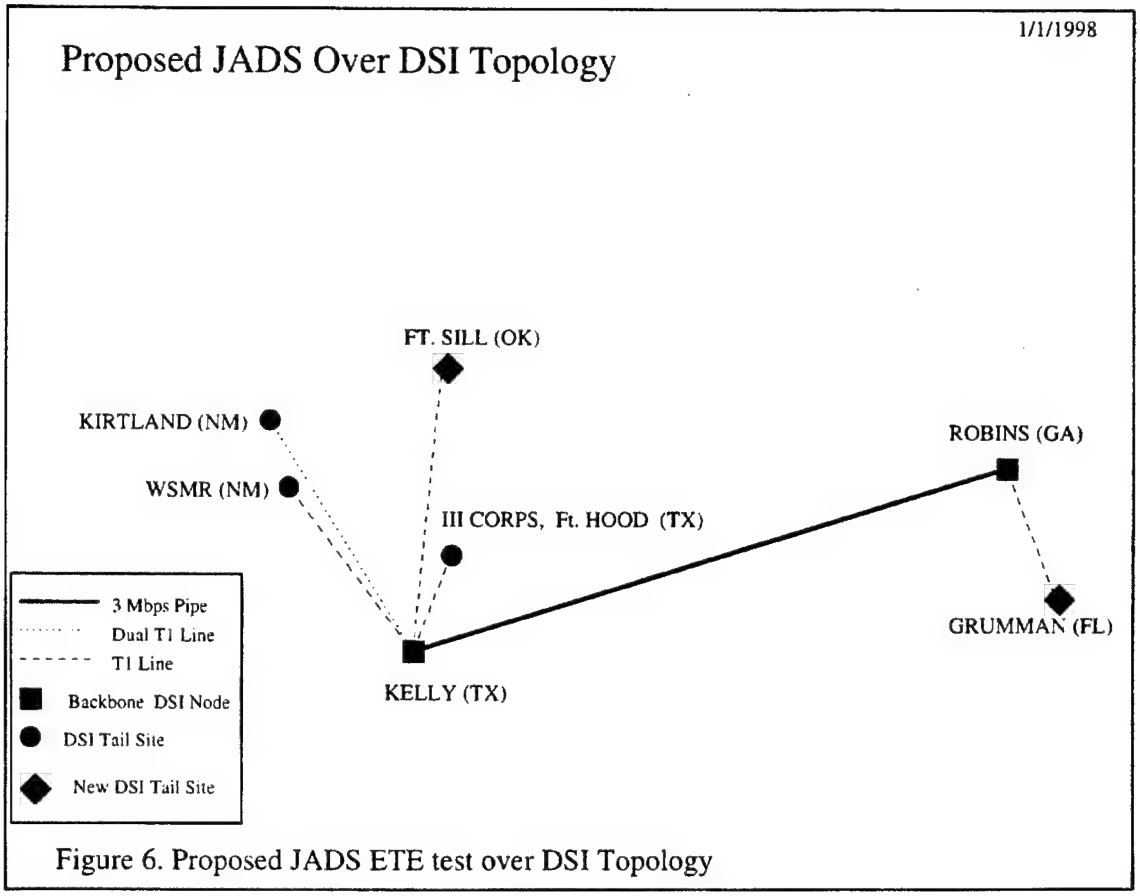


Figure 6. Proposed JADS ETE test over DSI Topology

The following assumptions have been made:

- The three existing DSI site nodes at WSMR, III Corps (Fort Hood), and KIRTLAND are available for JADS tests.
- Connectivity to two new DSI site nodes will exist. A new node at Fort Sill will be connected to the DSI backbone at KELLY. A new node at Grumman will be connected to the DSI backbone at ROBINS.

- The KIRTLAND node has a dual T1 link to KELLY. Inverse multiplexers are installed on the links between KELLY and KIRTLAND.
- Traffic in the backbone does not exceed 3 Mbps.
- The maximum latency in the backbone (measured by round-trip ping time) is 70 msecs. The maximum round-trip latency in the classified side (including INESs and aggregators) is assumed to be 100 msecs.
- Encryption is done by INESs. This is different from the KIV-7 encryption in JADS ETE tests.
- There exists a simulated SCDL link between the ground station at Grumman and the ground station at Fort Hood.

3.3 DSI SUPPORT OF JADS ETE PHASE 2 TESTS

Here we summarize the capabilities of the DSI and discuss the feasibility of the DSI to support JADS phase 2 ETE tests.

The DSI provides a robust network from which sites may be picked to participate in a JADS exercise. It provides a diverse community of sites to choose from. Standards based RSVP protocols on the DSI provide for bandwidth reservation. RSVP not only allows for latency bounds to be set up for packets, but also allows for efficient merging of reservations in a session. Bandwidth reservation is dynamic so that if a link goes down, traffic is automatically re-routed. Multicasting is supported so that packets in a distributed simulation are efficiently forwarded. Free internet tools such as VAT and VIC can be used for native multicasting among participating sites. Security is provided by INESs as discussed earlier. Network management tools allow for easy monitoring of the network.

JADS sites may be connected to the DSI to take advantage of the above features. However, there are costs associated with joining the DSI. These costs include equipment and monthly service charges. The equipment costs for two new sites is $120K. The circuit charges for the tail sites and the dual T1 line at KIRTLAND will be $27K per month. In addition the inverse multiplexers cost about $7K each. These costs may make running of JADS ETE test over the DSI uneconomical.

To run classified exercises, the limitations of the INESs need to be considered. The INES cannot match the link speed of a dedicated T1 link. The maximum throughput for large packets through the INES is about 1.2 Mbps in both directions.

Another serious problem arises if a site plans to continuously use the backbone links for an extended period of time and plans to run bandwidth intensive applications. With more than 50 sites and each backbone link having a capacity of 3 Mbps, a site may not be able to reserve

adequate bandwidth. Moreover, a site may not like the annoyance of scheduling and requesting bandwidth ahead of time.

To run video applications, the limitations of DVTC products should be considered. The DVTC products cannot be rated as excellent as far as performance is concerned. As mentioned earlier, there is considerable overhead in a DVTC session. This has an impact on performance, which JADS users may not be willing to accept.

Section 4

4. CONCLUSIONS

In this report we have presented a detailed review of the capabilities of modernized Phase II DSI. The topology of the DSI is presented. In addition, various capabilities of the DSI such as RSVP, multicasting, routing, VTC, security, and network management have been discussed. Information about the points of contact and the costs of joining the DSI have also been presented. Finally, possible future upgrade directions of the DSI have also been indicated. This information will be useful in making an informed decision on joining the DSI based on a particular group's requirements and budgets.

We also have considered a particular JADS ETE test scenario and the feasibility of running it over the DSI. A possible ETE test scenario over the DSI is presented. We listed the baseline requirements for running the JADS phase two ETE test on the DSI from what was observed in the actual test. We also discussed the feasibility of using DSI to support JADS phase two ETE test.

From a technical point of view, JADS ETE testing over the DSI is currently not a viable option. The main reason for this recommendation is the throughput limitations of the INES boxes. The two-way throughput for large packets (packet size of at least 1400 Bytes) is only 1200 Kilobits per second. From an economical point of view, the costs mentioned in the previous section may provide additional constraints for JADS to join the DSI. Finally, scheduling considerations may provide further annoyance for joining the DSI.

It is recommended that the issue of joining the DSI be revisited when DISA upgrades the INESs on the DSI to New INESs which are supposed to match the throughputs of T1 lines. At that time, there are no technical constraints expected for joining the DSI to link T&E simulations. The issue may be evaluated purely on an economic basis. It should be emphasized that the DSI provides robust standards-based state-of-the art IP protocols.

Appendix A

NORFOLK BACKBONE ROUTER CONFIGURATION

```
!
version 11.2
service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname NORFOLK
!
boot system flash slot0:rsp-pv-mz.112-6
enable secret XXXXXXXXXXX
!
ip subnet-zero
ip host lesd 199.57.66.2
ip host nor 199.57.64.94
ip host kel 199.57.64.114
ip host sco 199.57.64.122
ip host fpco 199.57.66.26
ip host col 199.57.64.98
ip host rob 199.57.64.102
ip host pen 199.57.64.93
ip host nisl 199.57.64.106
ip host ngic 199.57.66.38
ip host aatd 199.57.66.14
ip domain-name les.mil
ip name-server 199.57.127.70
ip name-server 199.57.127.150
ip multicast-routing
ip dvmrp route-limit 7000
!
interface ATM0/0
 mtu 9180
 no ip address
 ip pim dense-mode
 no ip mroute-cache
 ip rsvp bandwidth 5000 5000
 no ip route-cache optimum
```

```
!
interface ATM0/0.1 point-to-point
 description ATM Link to PENTAGON
 ip address 199.57.64.94 255.255.255.252
 ip pim dense-mode
 ip rsvp bandwidth 2250 2250
 atm pvc 1 0 101 aal5snap
 traffic-shape rate 3000000 75000 75000
!
interface ATM0/0.2 point-to-point
 description ATM Link to Robins
 ip address 199.57.64.101 255.255.255.252
 ip pim dense-mode
 ip rsvp bandwidth 2250 2250
 atm pvc 2 43 127 aal5snap
 traffic-shape rate 3000000 75000 75000
!
interface ATM0/0.3 point-to-point
 description ATM Link to North Island
 ip address 199.57.64.105 255.255.255.252
 ip pim dense-mode
 ip rsvp bandwidth 2250 2250
 atm pvc 3 39 125 aal5snap
 traffic-shape rate 3000000 75000 75000
!
interface Serial1/0/0
 no ip address
 ip rsvp bandwidth 1382 1382
 shutdown
 fair-queue 64 256 23
!
interface Serial1/0/1
 description Link to GUNTER
 ip address 199.57.64.21 255.255.255.252
 ip pim dense-mode
 ip rsvp bandwidth 1382 1382
 bandwidth 1544
 fair-queue 64 256 1000
!
interface Serial1/0/2
```

```
 description link to NGIC ccsd = 2820 ckt w36636/ds1-963441
 ip address 199.57.66.37 255.255.255.252
 ip pim dense-mode
 ip rsvp bandwidth 1382 1382
 bandwidth 1544
 fair-queue 64 256 1000
!
interface Serial1/0/3
 description link to LESD ccsd = 28ef ckt uhc504
 ip address 199.57.66.1 255.255.255.252
 ip pim dense-mode
 ip rsvp bandwidth 1382 1382
 bandwidth 1544
 fair-queue 64 256 1000
!
interface Serial4/0/0
 no ip address
 ip rsvp bandwidth 1382 1382
 bandwidth 1544
 shutdown
 fair-queue 64 256 1000
!
interface Serial4/0/1
 no ip address
 ip rsvp bandwidth 1382 1382
 bandwidth 1544
 shutdown
 fair-queue 64 256 1000
!
interface Serial4/0/2
 description link to AATD ccsd = 28q9 ckt 52hcga288710cv
 ip address 199.57.66.13 255.255.255.252
 ip pim dense-mode
 ip rsvp bandwidth 1382 1382
 bandwidth 1544
 fair-queue 64 256 1000
!
interface Serial4/0/3
 description lint to FPCO ccsd = 282U ckt w36645
 ip address 199.57.66.25 255.255.255.252
```

```
 ip pim dense-mode
 ip rsvp bandwidth 1382 1382
 bandwidth 1544
 fair-queue 64 256 1000
!
interface Serial4/1/0
 no ip address
 shutdown
!
interface Serial4/1/1
 no ip address
 shutdown
!
interface Serial4/1/2
 no ip address
 shutdown
!
interface Serial4/1/3
 no ip address
 shutdown
!
interface Serial5/0/0
 no ip address
 shutdown
!
interface Serial5/0/1
 no ip address
 shutdown
!
interface Serial5/0/2
 no ip address
 shutdown
!
interface Serial5/0/3
 no ip address
 shutdown
!
interface Serial5/1/0
 no ip address
 shutdown
```

```
!
interface Serial5/1/1
 no ip address
 shutdown
!
interface Serial5/1/2
 no ip address
 shutdown
!
interface Serial5/1/3
 no ip address
 shutdown
!
interface Ethernet6/0/0
 description Ethernet connection to JIS router
 ip address 198.26.132.42 255.255.255.252
 ip pim dense-mode
 load-interval 30
!
interface Ethernet6/0/1
 no ip address
 shutdown
!
interface Ethernet6/0/2
 no ip address
 shutdown
!
interface Ethernet6/0/3
 no ip address
 shutdown
!
router ospf 1
 redistribute bgp 3520
 network 199.57.64.20 0.0.0.3 area 0
 network 199.57.66.0 0.0.0.3 area 2
 network 199.57.65.108 0.0.0.3 area 2
 network 199.57.66.12 0.0.0.3 area 2
 network 199.57.64.92 0.0.0.3 area 0
 network 199.57.66.24 0.0.0.3 area 2
 network 199.57.64.104 0.0.0.3 area 0
```

```
 network 199.57.64.100 0.0.0.3 area 0
 network 199.57.64.24 0.0.0.3 area 0
 network 199.57.66.36 0.0.0.3 area 2
 default-information originate always
 area 0 range 199.57.64.0 255.255.255.0
 area 2 stub no-summary
 area 2 default-cost 110
!
router bgp 3520
 no synchronization
 network 199.57.64.0 mask 255.255.192.0
 network 199.57.128.0 mask 255.255.192.0
 neighbor 198.26.132.41 remote-as 568
!
ip classless
ip route 0.0.0.0 0.0.0.0 198.26.132.41
ip route 199.57.64.0 255.255.192.0 Null0
ip route 199.57.128.0 255.255.192.0 Null0
!
snmp-server community public RO
snmp-server community private RW
!
line con 0
line aux 0
 modem InOut
 transport input telnet
 stopbits 1
 rxspeed 19200
 txspeed 19200
 flowcontrol hardware
line vty 0 4
 password 7 08315E4B0D18111800
 login
!
end
```

Appendix B

JPSD SITE ROUTER CONFIGURATION

```
!
version 11.2
service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname JPSD
!
boot system flash slot0:c7200-p-mz.112-6
enable secret XXXXXXXXXXXXXXX
enable password XXXXXXXX
!
ip subnet-zero
ip domain-name les.mil
ip name-server 199.57.127.70
ip name-server 199.57.127.150
ip multicast-routing
ip dvmrp route-limit 7000
!
interface Loopback0
 no ip address
 no ip mroute-cache
 no ip route-cache
 shutdown
!
interface Ethernet1/0
 description Link to DVTC
 ip address 199.57.71.57 255.255.255.252
 ip pim dense-mode
 ip rsvp bandwidth 1382 1382
!
interface Ethernet1/1
 description Link to INES J3
 ip address 199.57.71.53 255.255.255.252
 ip pim dense-mode
 ip rsvp bandwidth 1382 1382
```

```
!
interface Ethernet1/2
 description Link to Unclass Sim
 ip address 199.57.146.1 255.255.255.0
 ip pim dense-mode
 ip rsvp bandwidth 1382 1382
!
interface Ethernet1/3
 no ip address
 ip pim dense-mode
 ip rsvp bandwidth 1382 1382
 shutdown
 fair-queue 64 256 1000
!
interface Serial2/0
 description link to N.ISLAND ccsd = 283k ckt mgs969320-151
 ip address 199.57.71.50 255.255.255.252
 ip pim dense-mode
 ip rsvp bandwidth 1382 1382
 bandwidth 1544
 fair-queue 64 256 1000
!
interface Serial2/1
 no ip address
!
interface Serial2/2
 no ip address
 shutdown
!
interface Serial2/3
 no ip address
 shutdown
!
router ospf 1
 passive-interface Ethernet1/0
 passive-interface Ethernet1/1
 passive-interface Ethernet1/2
 network 199.57.71.48 0.0.0.3 area 7
 network 199.57.71.52 0.0.0.3 area 7
 network 199.57.146.0 0.0.0.255 area 7
```

```
 network 199.57.71.56 0.0.0.3 area 7
 area 7 stub no-summary
!
ip classless
ip forward-protocol udp 3000
ip forward-protocol udp 3001
ip forward-protocol udp 3002
access-list 100 permit ip any any
!
snmp-server community public RO
!
line con 0
line aux 0
 modem InOut
 transport input telnet
 stopbits 1
 rxspeed 19200
 txspeed 19200
 flowcontrol hardware
line vty 0 4
 password 7 0314490E020E35435C
 login
!
end
```

Appendix C

JPSD RED ROUTER CONFIGURATION

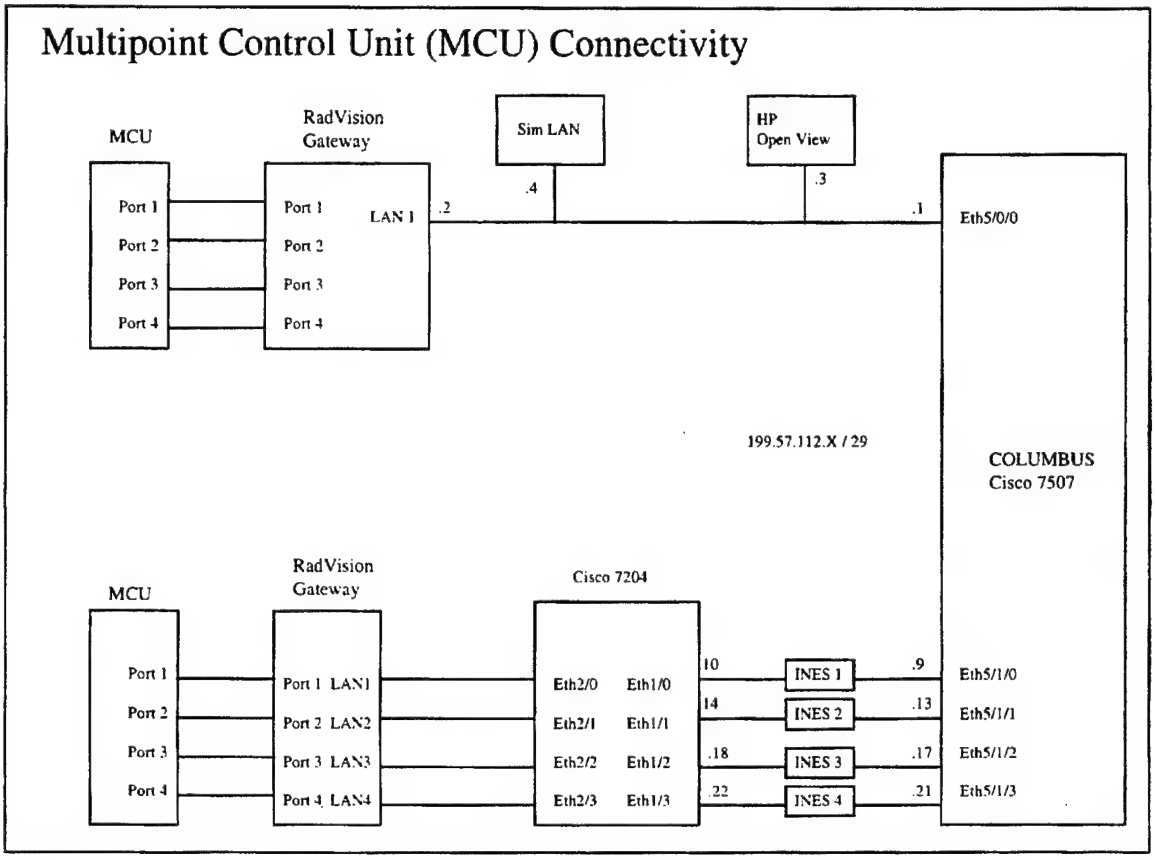
```
!
version 11.2
service udp-small-servers
service tcp-small-servers
!
hostname JPSD-4500
!
enable secret XXXXXXXXXXXXXXX
enable password xxxxx
!
ip subnet-zero
no ip domain-lookup
ip name-server 199.55.156.100
ip multicast-routing
ip dvmrp route-limit 7000
!
interface Ethernet0
 description Ethernet to Aggregator
 ip address 199.55.204.74 255.255.255.252
 ip pim dense-mode
 ip multicast helper-map 224.5.5.5 199.122.90.255 100
 ip igmp join-group 224.5.5.5
 media-type 10BaseT
!
interface Ethernet1
 description SIM-LAN
 ip address 199.122.90.1 255.255.255.0
 ip pim dense-mode
 ip multicast helper-map broadcast 224.5.5.5 100 ttl 10
 media-type 10BaseT
!
interface Ethernet2
 description DVTC-LAN
 ip address 199.55.204.77 255.255.255.252
 media-type 10BaseT
!
```

```
interface Ethernet3
 description Ethernet to INES
 ip address 199.55.204.67 255.255.255.248
 ip pim dense-mode
 load-interval 30
 media-type 10BaseT
!
interface Ethernet4
 no ip address
 shutdown
!
interface Ethernet5
 no ip address
 shutdown
!
ip classless
ip forward-protocol udp 4000
ip forward-protocol udp 4001
ip forward-protocol udp 3000
ip forward-protocol udp 3001
ip forward-protocol udp 3002
ip route 0.0.0.0 0.0.0.0 199.55.204.65
ip mroute 0.0.0.0 0.0.0.0 199.55.204.73
access-list 100 permit ip any any
tftp-server flash c4500-i-mz.112
!
line con 0
line aux 0
 transport input all

line vty 0 4
 exec-timeout 60 0
 password XXXXX
 login
!
end
```

Appendix D

COLUMBUS MCU



Appendix E

Columbus Control Center Personnel

Columbus Network Control Center Controller Information:

1. Mr. T. Brown, phone 614-692-6302, e-mail: tbrown@crcc.disa.mil
2. Mr. M. Boeck, phone 614-692-2223, e-mail: mboeck@crcc.disa.mil
3. Mr. J. Colley, phone 614-692-6320, e-mail: jcolley@crcc.disa.mil

Glossary

ADS	Advanced Distributed Simulation
ATM	Asynchronous Transfer Mode
ASCII	American Standard Code for Information Interchange
BBN	Bolt Beranek and Newman
BGP	Border Gateway Protocol
BSD	Berkeley System Distribution
CIDR	Classless Inter Domain Routing
CIK	Crypto Ignition Key
CN	Concentrator Node (a router product from Bay Networks)
DASU	DISN ATM Switch Unclassified
DIS	Distributed Interactive Simulation
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DSI	Defense Simulation Internet
DT&E	Developmental Test and Evaluation
DVTC	Desktop Video Teleconferencing
EIGRP	Enhanced IGRP (Cisco Systems Proprietary)
EPS	Enhanced Product Server
ETE	End-to-end
EW	Electronic Warfare
ff	Fixed Filter (a reservation style in RSVP)
HLA	High Level Architecture
IETF	Internet Engineering Task Force
IGMP	Internet Group Membership Protocol
IGRP	Inter-gateway Routing Protocol (Cisco Systems Proprietary)
INES	Improved Network Encryption System
IP	Internet Protocol
ISDN	Integrated Services Digital Network
JADS	Joint Advanced Distributed Simulation
JIS	Joint Information Services

JPSD	Joint Precision Strike Demonstration
JSTARS	Joint Surveillance Target Attack Radar System
Kbps	Kilobits per second
KSD	Key Storage Device
LAN	Local Area Network
LN	Link Node (
Mbps	Megabits per second
MCU	Multipoint Control Unit
ModSAF	Modular Semi-Automated Forces
NCC	Network Control Center
NSA	National Security Agency
NVROM	Non-volatile Read-Only Memory
OSD	Office of the Secretary of Defense
OSPF	Open Shortest Path First
OT&E	Operational Test and Evaluation
PC	Personal Computer
PIM	Protocol Independent Multicasting
PVC	Permanent Virtual Circuit
QOS	Quality of Service
RFC	Request for Comment
RSVP	Resource ReSerVation Protocol
SIT	Systems Integration Test
ST II	Streams Protocol, Version II
STAR	Surveillance Target Attack Radar System
T1	System that transports Digital Signal Level 1 (1.544 Mbps)
T&E	Test and Evaluation
TCAC	Test, Control, and Analysis Center
ttl	time to live
UDP	User Datagram Protocol

VAT	A Free Audio-conferencing Tool
VCI	Virtual Channel Identifier
VIC	A Free Video-conferencing Tool
VPI	Virtual Path Identifier
VTC	Video Teleconferencing
WB	White Board
wf	Wild-card filter (a reservation style in RSVP)
WSMR	White Sands Missile Range

Distribution List

Internal

W010

J. S. Quilty

W110

J. C. Slaybaugh

W150

H. J. Carpenter
R. Eftekari

W15D

J. S. Dahmann

W15E

C. E. Walters (5)
E. R. Gonzalez
G. A. Tsoucalas
F. R. Richards
M. Hammond
Files (2)

W15F

M. Adams
S. Chakravorty
D. Sahu (5)
N. Schult

W062

N. J. Slattery
S. Welman

Records Resources (3)

External

Office of the Under Secretary of Defense
(Acquisition)
Deputy Director, Test,, systems Engineering &
Evaluation/Systems Assessment
ATTN: Lt. Col. Steven Cameron
The Pentagon, Room 3D1080
Washington, DC 20301-3110 (5)

Colonel Mark Smith
JADS Joint Test Director
JADS JTF
11104 Menaul Blvd., NE
Albuquerque, NM 87112 (10)